ELEMENTS OF ORDER P IN THE TATE-ŠAFAREVIČ GROUP

J. S. MILNE

By a global field, we will always mean a number field or a function field in one variable over a finite field. Lang and Tate have shown [4] that the Tate-Šafarevič group of an abelian variety over such a field has only finitely many elements of order dividing a fixed integer m, provided that m is not divisible by the characteristic p of the field. The purpose of this note is to remove the restriction on m. Our proof is complicated by the fact that, unlike the prime-to-p case, there may be an infinite number of principal homogeneous spaces of order p over the global field which split locally at all primes outside a given non-empty finite set, and hence we must work with all the primes of K.

THEOREM. *For any abelian variety A over a global field K, and any integer m, the Tate-Šafarevič group $\text{Ш}(A/K)$ of A over K has only finitely many elements of order dividing m.*

After [4; Theorem 5], we may assume that K has non-zero characteristic p, and that $m = p$. As in the proof of the above-cited theorem, we may replace K by a finite separable extension and hence assume that the kernel of the isogeny $p : A \to A$ (as a finite group scheme) has a composition series whose quotients are one of the three group schemes $\mathbb{Z}/p\mathbb{Z}$, $\boldsymbol{\alpha}_p$, $\boldsymbol{\mu}_p$ [6]. Correspondingly, $p : A \to A$ will be a composite of isogenies, $p = \phi_{2d} \circ \phi_{2d-1} \circ \ldots \circ \phi_1$, $\phi_i : A_{i-1} \to A_i$, with all the ϕ_i of degree p. Thus, it suffices to prove the statement: let $\phi : A \to B$ be an isogeny over K with kernel equal to one of $\mathbb{Z}/p\mathbb{Z}$, $\boldsymbol{\alpha}_p$, or $\boldsymbol{\mu}_p$. Then the kernel of the map

$$\text{Ш}(\phi) : \text{Ш}(A/K) \to \text{Ш}(B/K),$$

induced by ϕ is finite.

We will write $H^i(S, -)$ for a cohomology group with respect to the flat (*f. p. q. f.*) topology on S (or spec S if S is a ring), X for the complete, smooth algebraic curve canonically associated to K/k, and X_0 for the set of closed points of X (i.e. primes of K). If v is in X_0, then K_v is the completion of K at v and R_v the ring of integers in K_v. All of our group schemes will be commutative.

If G is a group scheme of finite type over K_v, then there is a canonical topology on $H^i(K_v, G)$ [6]. Let $\mathcal{N}$ be a finite flat group scheme over R_v and let $N = \mathcal{N} \otimes_{R_v} K_v$. Then the canonical map $H^1(R_v, \mathcal{N}) \to H^1(K_v, N)$ is injective, because a principal homogeneous space for $\mathcal{N}$ over R_v which has a point in K_v clearly already has a point in R_v. Thus, any element of $H^1(R_v, \mathcal{N})$ is split by the integral closure R_v' of

Received 23 February, 1970. This research was supported by the Office of Naval Research.

[BULL. LONDON MATH. SOC., 2 (1970), 293–296]

R_v in a finite extension field of K_v, and $H^1(R_v, \mathcal{N})$ may be identified with the Cech cohomology group $\varinjlim H^1(R_v'/R_v, \mathcal{N})$ where the limit runs over all such R_v'. It follows easily from this that $H^1(R_v, \mathcal{N})$ is embedded as an open subgroup of $H^1(K_v, N)$.

Now let N be a finite group scheme over K. There is an open subscheme U of X and a finite flat group scheme $\mathcal{N}$ over U such that $\mathcal{N} \times_U \operatorname{spec} K = N$ (if $N = \operatorname{spec} S$ then, locally $\mathcal{N}$ is described by a lattice in S which is stable under the map $\delta : S \to S \otimes S$ giving the multplication in N). We define $\Pi' H^1(K_v, N)$ to be the restricted topological product of the groups $\left(H^1(K_v, N)\right)_{v \in X_0}$ with respect to the family of open subgroups $\left(H^1(R_v, \mathcal{N}_v)\right)_{v \in U_0}$, where $\mathcal{N}_v = \mathcal{N} \times_U \operatorname{spec} R_v$. Then $\Pi' H^1(K_v, N)$ is independent of the pair $(\mathcal{N}, U)$, for if $(\mathcal{N}', U')$ is any other such pair there is an open subscheme of $U \cap U'$ on which $\mathcal{N}$ and $\mathcal{N}'$ are isomorphic.

LEMMA 1. *Let N be one of the group schemes $\mathbb{Z}/p\mathbb{Z}$, α_p, μ_p. Then the canonical maps $\alpha_v : H^1(K, N) \to H^1(K_v, N)$ define an injection $\alpha : H^1(K, N) \to \Pi' H^1(K_v, N)$, and the image of α is a discrete subgroup of $\Pi' H^1(K_v, N)$.*

Proof. The maps α_v can be identified with, respectively, the maps

$$K/\wp K \to K_v/\wp K_v$$

$$K/K^p \to K_v/K_v{}^p$$

$$K^*/K^{*p} \to K_v{}^*/K_v{}^{*p}$$

induced by the inclusion of K in K_v. In defining the restricted topological product $\Pi' H^1(K_v, N)$ we may take $\mathcal{N}$ to be $\mathbb{Z}/p\mathbb{Z}$ (resp. α_p, μ_p) regarded as a group scheme over X. Then the image of any element of $K/\wp K$ (resp. K/K^p, K^*/K^{*p}) is contained in $H^1(R_v, \mathbb{Z}/p\mathbb{Z}) = R_v/\wp R_v$ (resp. $H^1(R_v, \alpha_p) = R_v/R_v{}^p$, $H^1(R_v, \mu_p) = R_v{}^*/R_v{}^{*p}$) for almost all v. Thus the α_v do define a map $\alpha : H^1(K, N) \to \Pi' H^1(K, N)$, and α is injective by class field theory [**1**; p. 12, Th. 2; p. 82, Th. 1]. $\Pi' H^1(K_v, \mathbb{Z}/p\mathbb{Z})$ is isomorphic, both topologically and algebraically, to the adele group V of K modulo its closed subgroup $\wp V$. Hence im (α) is isomorphic to $(K + \wp V)/\wp V$, and we must show that $\wp V$ is an open subgroup of $K + \wp V$. Let $V(0)$ be the open subgroup ΠR_v of V, and let $M = \left(V(0) + \wp V\right) \cap K$. Then [*cf.* **1**; p. 23] $M/\wp K$ is dual to the Galois group of the maximal abelian unramified extension of K of exponent p, and this is finite. Hence $\wp V$ is open in $M + \wp V$ (because it is closed and of finite index) and $M + \wp V = \left(V(0) + \wp V\right) \cap (K + \wp V)$ is open in $K + \wp V$.

Similarly, the second case reduces to showing that if $M = \left(V(0) + V^p\right) \cap K$, then M/K^p is finite. If $a \in M$, $a = \alpha + \beta^p$ $(\alpha \in V(0), \beta \in V)$ define

$$i(a) = \bar{\beta} \in V/\left(V(0) + K\right).$$

Then i is a well-defined map $M \to V/\left(V(0) + K\right)$ with kernel K^p, and $V/\left(V(0) + K\right)$ is well-known to be finite.

The third case may be proved similarly using the ideles instead of the adeles.

LEMMA 2. *Let $N = \ker(\phi)$, and let $\beta_v : B(K_v) \to H^1(K_v, N)$ be the map in the cohomology sequence arising from $0 \to N \to A \xrightarrow{\phi} B \to 0$. Then the β_v define a map $\beta : \prod_{v \in X_0} B(K_v) \to \Pi' H^1(K_v, N)$, and the image of β is compact.*

Proof. There is an open subscheme U of X and an isogeny $\tilde{\phi} : \mathscr{A} \to \mathscr{B}$ of abelian schemes over U such that $\tilde{\phi}_{(K)} = \phi$. Let $\mathscr{N} = \ker(\tilde{\phi})$ and let $v \in U_0$. There is an exact commutative diagram

$$\begin{array}{ccccc} \mathscr{B}(R_v) & \to & H^1(R_v, \mathscr{N}) & \to & H^1(R_v, \mathscr{A}) \\ \downarrow & & \downarrow & & \downarrow \\ B(K_v) & \to & H^1(K_v, N) & \to & H^1(K_v, A) \end{array}$$

where the rows are the cohomology sequences of the short exact sequences

$$0 \to \mathscr{N} \to \mathscr{A} \to \mathscr{B} \to 0,$$

and

$$0 \to N \to A \to B \to 0,$$

respectively.

The first vertical arrow is an isomorphism, and $H^1(R_v, \mathscr{A}) = 0$ [2; Th. 11.7; 3], and hence β_v maps into the subgroup $H^1(R_v, \mathscr{N})$ of $H^1(K_v, N)$ for all $v \in U_0$. This shows that the β_v define a map β as required.

Each β_v is continuous with respect to the canonical topologies on the cohomology groups. Indeed, let K' be a finite extension of K and consider the exact commutative diagram

$$\begin{array}{ccccccc} 0 \to & N(K') & \to & A(K') & \xrightarrow{\phi} & B(K') \\ & \downarrow & & \downarrow \delta & & \downarrow \\ 0 \to & N(K' \otimes_K K') & \to & A(K' \otimes_K K') & \to & B(K' \otimes_K K') \end{array}$$

All of the maps are continuous because they are given by polynomials. $N(K' \otimes_K K')$ has the subspace topology induced by that of $A(K' \otimes_K K')$, and ϕ is an open map onto its image. It follows that the inverse image (under β_v) of any open subset of $H^1(K'/K, N)$ is open in $\{b \in B(K) \mid \exists\, a \in A(K'), \phi(a) = b\}$. The required continuity follows now by taking unions over all such K'. The continuity of the β_v imply that of β, and the compactness of the $B(K_v)$ imply that of $\Pi B(K_v)$ and hence of its image in $\Pi' H^1(K_v, N)$.

We may now prove the theorem. Consider the commutative diagram:

$$\begin{array}{ccccc} B(K) & \to & H^1(K, N) & \to & H^1(K, A) \\ \downarrow & & \downarrow \alpha & & \downarrow \\ \Pi B(K_v) & \to & \Pi' H^1(K_v, N) & \to & \Pi H^1(K_v, A) \end{array}$$

We will show that the inverse image $S^{(\phi)}$ of $\ker(\coprod(\phi))$ in $H^1(K, N)$ is finite. By Lemma 1, $\alpha(S^{(\phi)})$ is isomorphic to $S^{(\phi)}$, but $\alpha(S^{(\phi)})$ is the intersection of a compact subgroup $\operatorname{im}(\beta)$, with a discrete (and closed) subgroup $\operatorname{im}(\alpha)$, and hence is finite.

We now give an example to illustrate the fact that in general, if A is an abelian variety over a global field K of characteristic p, and S is a non-empty finite subset of X_0, then

$$H^1(K, A, S) = \ker\left(H^1(K, A) \to \prod_{v \in X_0,\, v \notin S} H^1(K_v, A)\right)$$

has infinitely many elements of order p. Choose $K = k(X)$, a pure transcendental extension of the finite field k, and choose A to be an abelian variety which has good reduction everywhere except possibly at the prime v_∞ corresponding to X^{-1}. A comes from an abelian scheme $\mathscr{A}$ on $U = \operatorname{spec} k[X]$, and if $S = \{v_\infty\}$, then $H^1(K, A, S) = H^1(U, \mathscr{A})$ [5; p. 98; Lemma 1]. Moreover, assume that the kernel of multiplication by p on $\mathscr{A}$ has a composition series among whose quotients are a $\mathbb{Z}/p\mathbb{Z}$ or an α_p (such abelian varieties do exist; consider for example, constant abelian varieties). Then $H^1(K, A, S)$ has finitely many elements of order p if and only if $H^1(U, \mathbb{Z}/p\mathbb{Z})$ (or $H^1(U, \alpha_p)$) is finite. But $H^1(U, \mathbb{Z}/p\mathbb{Z}) = k[X]/\wp k[X]$ and

$$H^1(U, \alpha_p) = k[X]/k[X]^p,$$

which are both infinite.

It is also easy to give examples of abelian varieties over function fields in one variable over algebraically closed fields whose Tate-Šafarevič groups have infinitely many elements of order p.

References

1. E. Artin and J. Tate, *Class field theory* (Harvard, 1961).
2. A. Grothendieck, " Le groupe de Brauer III ", in *Dix Exposes sur la cohomologie des Schemas* (North-Holland, Amsterdam; Masson, Paris, 1968).
3. S. Lang, " Algebraic groups over finite fields ", *Amer. J. Math.*, 78 (1956), 555–563.
4. S. Lang and J. Tate, " Principal homogenous spaces over abelian varieties ", *Amer. J. Math.*, 80 (1958), 659–684.
5. J. Milne, " The Tate-Šafarevič group of a constant abelian variety ", *Inventiones math*, 6 (1968), 91–105.
6. S. Shatz, " Cohomology of artinian group schemes over local fields ", *Ann. of Math.*, 79 (1964), 411–449.

University of Michigan.